

[| NODIS Library](#) | [Legal Policies\(2000s\)](#) | [Search](#) |

# NASA Procedural Requirements

**COMPLIANCE IS MANDATORY****NPR 2810.1A**Effective Date: May  
16, 2006Expiration Date: May  
16, 2016[Printable Format \(PDF\)](#)

Request Notification of Change

(NASA Only)

**Subject: Security of Information Technology (Revalidated with  
Change 1, dated May 19, 2011)****Responsible Office: Office of the Chief Information Officer**[| TOC](#) | [ChangeHistory](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) |  
[Chapter4](#) | [AppendixA](#) | [AppendixB](#) | [AppendixC](#) | [AppendixD](#) | [AppendixE](#) |  
[ALL](#) |

## Chapter 2 - Management Controls

### 2.1 Program Management (PM)

2.1.1 The Program Management control family relates to the legal requirements that NASA develop, document, and implement a comprehensive program under the direction of senior management, to provide security for information and information systems. The information security program is required to include ongoing assessments of the risk and magnitude of the harm that could result from compromise to Agency information systems' confidentiality, integrity, and availability. Such risk assessments, when addressed throughout the information system life cycle, can cost-effectively help to reduce information security risks.

2.1.2 The tenets and framework of NASA's information security program are spelled out in this NPR and its referenced security handbooks. The policies, procedures, milestones, metrics, and responsibilities of the information security program together make up the information security program plan.

#### 2.1.3 Program Management Policy

##### 2.1.3.1 The NASA CIO shall:

- a. Report periodically to the NASA Administrator on the effectiveness of NASA's information security program, including the progress of remedial actions.
- b. Ensure the development and maintenance of a NASA-wide information system

inventory.

c. Report to OMB on the status of NASA's information security program, as required.

#### 2.1.3.2 The SAISO shall:

a. Develop and document a NASA-wide information security program which includes an overview and descriptions of measures of performance, enterprise security architecture, critical infrastructure, risk management strategy, and an information security assessment and authorization process.

b. Continuously review, update, and augment the information security program as necessary.

c. Ensure that the information security program plan, policy, and requirements are implemented.

d. Define a process for the development, documentation, and maintenance of plans of action and milestones (POA&M) and for the acceptance of risk.

e. Establish and manage a NASA-wide information security performance metrics program.

f. Coordinate information security reviews with the NASA Office of the Inspector General (OIG) and other external entities such as the U.S. Government Accountability Office (GAO).

## 2.2 Security Assessment and Authorization (CA)

2.2.1 The Security Assessment and Authorization control family relates to the activities and requirements surrounding the routine testing of security controls, the continuous monitoring of system security posture, and the ongoing risk-based decisions to approve or deny the use of a system. Officials within the NASA community are responsible for continuously ensuring the effectiveness of security control implementations throughout the life cycle of a system. Moreover, in light of an ever-changing security landscape, designated NASA officials should always be prepared to determine the impact of a system's operation on the success of the NASA mission.

2.2.2 Security Assessment and Authorization procedures shall be governed by ITS-HBK-2810.02, Security Assessment and Authorization.

#### 2.2.3 Security Assessment and Authorization Policy

2.2.3.1 The NASA CIO shall ensure information security control assessments, security authorizations, and OMB and FISMA reporting directives are completed across the Agency in a timely and cost-effective manner.

#### 2.2.3.2 The SAISO shall:

a. Ensure the assessment, updating, and dissemination of information regarding Agency Common Controls.

b. Ensure the assessment, updating, and dissemination of information regarding those portions of Hybrid Controls which the Agency implements.

c. Ensure the annual updating and dissemination of Organizationally-Defined Values via

an OCIO memorandum or handbook update.

- d. Provision a NASA-wide repository for information security documentation.
- e. Ensure the identification and management of common threats to NASA.
- f. Ensure compliance with OMB and FISMA reporting requirements.

#### 2.2.3.3 The Center CISO shall:

- a. Verify the proper application of information system categorization criteria and requirements.
- b. Ensure the identification and management of common threats to their Center.

#### 2.2.3.4 The OCSO shall:

- a. Verify the proper application of information system categorization criteria and requirements for their organization.
- b. Ensure the identification and management of common threats to their organization.

#### 2.2.3.5 The AO shall:

- a. Ensure that all systems undergo a complete system security assessment prior to granting an initial ATO.
- b. Approve or reject information system categorizations.
- c. Grant or deny systems ATO based on an evaluation of risk to the security posture of their information systems.
- d. Make decisions with regard to the planning and resourcing of information security assessment and authorization activities.

#### 2.2.3.6 The ISO shall:

- a. Ensure capabilities to continuously monitor the security posture of their information system.
- b. Ensure the creation of POA&Ms, or provide a documented acceptance of risk related to any identified system security deficiencies or weaknesses.
- c. Ensure the maintenance of security documentation in the NASA-wide security document repository.
- d. Maintain and update formal documentation regarding system interconnections.
- e. Ensure the availability of resources for assessment and authorization activities.
- f. Ensure the completion of POA&M items.
- g. Inform key officials of pending assessment and authorization activities.
- h. Seek an ATO from the AO prior to the operation of a new system, and maintain an ongoing authorization thereafter, in accordance with a risk-based approach to security.

2.2.3.7 The IO shall categorize information and ensure, in collaboration with the ISO, that information system categorizations appropriately reflect the information they generate, collect, process, and disseminate.

## 2.3 Planning (PL)

2.3.1 The Planning control family relates to the definition and documentation of the key resources and activities used to protect Agency information system resources. Effective security planning is both comprehensive and flexible. NASA uses a System Security Plan (SSP) template that specifies the set of information controls that must be considered for each system. The plan content for any specific system is governed by a risk assessment of the particular threats facing the system and a tailoring of security controls to meet those threats.

2.3.2 NASA follows the requirements of FIP 199, Standards for Security Categorization of Federal Information and Information Systems.

2.3.3 Security Planning procedures shall be governed by NPR 1382.1, NASA Privacy Procedural Requirements; ITS-HBK-2810.03, Planning.

### 2.3.4 Planning Policy

2.3.4.1 The SAISO shall identify a NASA-wide resource for the management of corrective action plans to mitigate information system security weaknesses.

2.3.4.2 The OCSO shall ensure that their organization's SSPs are reviewed and updated in accordance with this NPR and its associated handbooks.

2.3.4.3 The AO shall approve SSPs under their authority.

2.3.4.4 The ISO shall:

- a. Ensure that all SSPs are developed and tailored to address the threats and associated risks faced by the system.
- b. Develop Memoranda of Agreements (MOA), Memoranda of Understandings (MOU), and Interconnection Security Agreements (ISA) for their systems as applicable.
- c. Develop and maintain a SSP for their information systems.
- d. Ensure that SSPs are reviewed and updated in accordance with this NPR and its associated handbooks.
- e. Establish rules of behavior for their systems as required.

## 2.4 Risk Assessment (RA)

2.4.1 The Risk Assessment control family relates to a framework for the identification, tracking and mitigation of information security risks. The goal of effective risk management is to articulate the risk that threats may have on Agency owned assets, data and personnel, and to minimize the risk by applying security controls.

2.4.2 In order to make informed decisions about the security of Agency assets and personnel, all Agency security roles share the responsibility of understanding the risks that affect their information and information systems, and the mitigating controls which address them. All roles are responsible for communicating risks to the level necessary to satisfy all potential stakeholders.

2.4.3 NASA utilizes the guidelines of NIST SP 800-30, Risk Management Guide for

Information Technology Systems; and NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems.

2.4.4 Risk Assessment procedures shall be governed by NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements; NPR 8000.4, Agency Risk Management Procedural Requirements; and ITS-HBK-2810.04, Risk Assessment.

#### 2.4.5 Risk Assessment Policy

2.4.5.1 The SAISO shall define and make available a RMF that describes a uniform methodology for risk assessment that is applicable to all Agency internal and external systems.

2.4.5.2 The Center CISO shall understand and communicate, with the AO and ISO, any risks associated with any information system which may pose an unacceptable level of risk to Agency operations and resources.

2.4.5.3 The AO shall ensure that only systems posing an acceptable level of risk to Agency assets, data, and personnel are approved for production operation.

2.4.5.4 The ISO shall:

- a. Ensure that their information systems are assessed for risk in accordance with Agency policy and procedures.
- b. Ensure resources are applied towards the mitigation of identified risks to minimize risk.
- c. Ensure that systems that are identified as posing unacceptable risk to other Agency operations or resources are communicated to the Center CISO and AO and mitigated in a manner that ensures the protection of Agency assets, data, and personnel.

## 2.5 System and Services Acquisition (SA)

2.5.1 The System and Services Acquisition control family relates to the need to adequately plan for, appropriately fund, and efficiently acquire the resources necessary to maintain information security. The control family defines the actions that best enable NASA's security program to make effective use of externally-sourced expertise and tools. Furthermore, it mandates that security considerations not be treated as an afterthought, but are instead addressed early-on in parallel with funding and design decisions.

2.5.2 System and Services Acquisition procedures shall be governed by ITS-HBK-2810.05, System and Services Acquisition.

#### 2.5.3 System and Services Acquisition Policy

2.5.3.1 The SAISO shall:

- a. Include information security resource requirements in programming and budgeting documentation.
- b. Work with the NASA Office of Procurement to oversee the development and maintenance of an information security clause and coordinate its implementation in the NASA Federal Acquisition Regulations (FAR) with the NASA Office of Procurement.

### 2.5.3.2 The ISO shall:

- a. Ensure that required System and Services Acquisition policy and procedures are implemented for their information systems and documented in the associated SSPs.
- b. Ensure information security considerations are managed throughout their systems' development life cycle.
- c. Ensure that the appropriate information security requirements are articulated in solicitations and resulting contracts for acquisitions made in support of their systems.  
Note: The principal information security clause to be included with contracts, grants, and other agreements is defined by the FAR clause and applicable Procurement Information Circular IT Security Requirements.

2.5.3.3 The IO shall assist in the development of security requirements for inclusion in solicitations and resulting contracts for acquisitions made in support of their information.

2.5.3.4 The ISSO shall assist in the development of security requirements for inclusion in solicitations and resulting contracts for acquisitions made in support of their information systems.

2.5.3.5 The Assistant Administrator of Procurement shall:

- a. Ensure that contracting officials are aware of requirements related to information security.
- b. Ensure the inclusion of information security requirements in all contracts and solicitations.

[TOC](#)	[ChangeHistory](#)	[Preface](#)	[Chapter1](#)	[Chapter2](#)	[Chapter3](#)
[Chapter4](#)	[AppendixA](#)	[AppendixB](#)	[AppendixC](#)	[AppendixD](#)	
[AppendixE](#)	[ALL](#)				

| [NODIS Library](#) | [Legal Policies\(2000s\)](#) | [Search](#) |

### **DISTRIBUTION:** **NODIS**

---

#### **This Document Is Uncontrolled When Printed.**

Check the NASA Online Directives Information System (NODIS) Library  
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>

---